Norton AntiVirus™ for Microsoft Exchange

Symantec™

NORTON
AntiVirus™
FOR MICROSOFT® EXCHANGE

Norton AntiVirus™ for Microsoft Exchange

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Documentation Version 2.1

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

Trademarks

Symantec, the Symantec logo, Norton AntiVirus, LiveUpdate, Striker, Bloodhound, and Symantec AntiVirus Research Center (SARC) are trademarks of Symantec Corporation.

Microsoft, Windows, and Windows logo are registered trademarks, and Microsoft Exchange is a trademark of Microsoft Corporation. NetWare is a registered trademark of Novell, Inc. Mac and Mac OS are trademarks of Apple Computer, Inc. Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

(i) use only one copy of one version of the various versions of the Software contained on the enclosed CD-ROM on a single computer;
(ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
(iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
(iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
(v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

You may not:

(i) copy the documentation which accompanies the Software;
(ii) sublicense, rent or lease any portion of the Software;
(iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
(iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.
THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you
accept the Software.

U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

SYMANTEC LICENSE AND WARRANTY

Notwithstanding any of the terms and conditions contained in the Symantec Software License, you may make and use up to that number of copies of the Software that is indicated on the License Authorization Coupon contained in your box. The coupon will constitute proof of your right to make and use such additional copies.

CONTENTS

Norton AntiVirus for Microsoft Exchange

Service and support solutions

CD Replacement Form

Index

Norton AntiVirus for Microsoft Exchange

Norton AntiVirus secures your Microsoft Exchange environment against virus attack by monitoring all public folders and mailboxes on your Exchange servers. Norton AntiVirus operation is transparent to users, with minimal performance degradation to the network.

The Microsoft Exchange environment is only one avenue a virus can use to penetrate your site. For a complete virus protection solution, make sure the appropriate workstation or server version of Norton AntiVirus is installed on every computer at your site as well.

About Norton AntiVirus

Norton AntiVirus scans message bodies and attachments sent to mailboxes and public folders on Microsoft Exchange servers, including files in compressed and encoded formats, such as MIME and ZIP.

Through its HyperText Markup Language (HTML) user interface you view processing statistics, examine the Activity Log that records all Norton AntiVirus events, manage the Quarantine that stores items withheld from delivery, and configure operation—either from the physical server or remotely from any workstation on the network.

With the Norton AntiVirus Auto-Protect feature, viruses are detected in real time as email and messages are routed through the Microsoft Exchange server. If a virus is detected, Norton AntiVirus can be configured to do any of the following:

- Repair infected attachments to eliminate viruses automatically on detection.
- Quarantine infected attachments for administrator review.

- Delete infected attachments.
- Continue delivery, but log the virus detection.

When viruses are detected, email notifications are sent, optionally, to specified administrators. In addition, Windows NT alerts can be sent to specified machines and users. If Norton AntiVirus for Windows NT is running on the network, alerts can be sent to the Norton AntiVirus alert service.

What is a computer virus?

A computer virus is a program designed in such a way that, when run, it attaches a copy of itself to another computer program or document. Thereafter, whenever the infected program is run or the document is opened, the attached virus program is activated and attaches itself to yet other programs and documents.

In addition to replicating, viruses are generally programmed to deliver a payload. Most viruses simply display a message on a particular trigger date. Some, however, are programmed specifically to damage data by corrupting programs, deleting files, or reformatting disks.

Two classes of viruses present the greatest threat in the Microsoft Exchange environment:

- Macro viruses infect word processing and spreadsheet documents.
- Program viruses infect executable files.

The viruses spread as attachments to email and messages routed through Microsoft Exchange servers. Norton AntiVirus for Microsoft Exchange detects and eliminates these viruses.

How Norton AntiVirus works

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. Once a virus is identified, information about the virus (a virus signature) is stored in a virus definitions file, which contains the necessary information to detect and eliminate the virus. When Norton AntiVirus scans for viruses, it is searching for these telltale virus signatures.

To supplement detection of known viruses, Norton AntiVirus includes a powerful component called Bloodhound. With this advanced heuristic technology, Norton AntiVirus can detect a high percentage of new or unknown viruses not yet analyzed by antivirus researchers.

The Norton AntiVirus LiveUpdate feature makes sure your virus protection remains current. Updated virus definitions files are available from Symantec regularly. With LiveUpdate, Norton AntiVirus connects automatically to a special Symantec site, determines if your files need updating, downloads the proper files, and installs them in the proper location.

Scanning modes

Previous versions of Norton AntiVirus for Microsoft Exchange used the Microsoft Messaging API (MAPI) to scan traffic for viruses. Microsoft Exchange Server 5.5 with Service Pack 3 or later (including Exchange 2000) adds the new Microsoft Virus Scanning API (VAPI).

VAPI functionality is vastly different from MAPI. VAPI will guarantee that an attachment is scanned before a user can access the attachement. The VAPI solution is also a more efficient approach for virus scanning and should have less impact on the server's performance.

VAPI, however, does not offer a great level of detail when it comes to determining the source of an attachment with an infection. The only information that will be reported is the attachment name. There is no information about the sender, recipient, message subject, or message location. These limitations prevent Norton AntiVirus from sending notifications to the sender and recipients of infected messages.

When VAPI is enabled, all attachments in the information store are scanned. There are no options to control which mailboxes or file types are to be scanned, as all attachments are scanned. Manual and scheduled scans of mailboxes and public folders are no longer necessary with the VAPI solution, as there is no way to retrieve an unscanned attachment from the Exchange information store. A configuration option enables background scanning of the entire Exchange information store.

With this new capability, Norton AntiVirus for Microsoft Exchange can be configured to run in one of three different modes, which can be selected at install or as a configuration choice after install.

- MAPI mode: Uses the Messaging API (MAPI) that was used for previous versions of Norton AntiVirus for Microsoft Exchange. It logs into each protected mailbox and scans new mail as it arrives in the mailbox's inbox. This mode must be selected for earlier versions of Microsoft Exchange.
- VAPI mode: Uses the new Virus Scanning API (VAPI) in Exchange 5.5 Service Pack 3. VAPI is used to scan every attachment as it is saved or

loaded from the Exchange information store. There is no information, however, about the sender, recipient, message subject, or message location. These limitations prevent Norton AntiVirus for Microsoft Exchange from sending notifications to the sender and recipients in this mode. Notifications, however, are sent to administrators.

- MAPI/VAPI combination mode: Uses both MAPI and VAPI technologies. It uses VAPI to guarantee that all attachments are scanned, and it uses MAPI to determine more information about the source of an attachment for logging, alerting, and reporting.

For earlier versions of Microsoft Exchange that do not include VAPI, MAPI mode must be used. For later versions, the VAPI/MAPI combination mode is recommended. If server demand is very high and performance is critical, the VAPI only mode is suggested.

Installing Norton AntiVirus for Microsoft Exchange

Minimum system requirements

Norton AntiVirus for Microsoft Exchange runs under Windows NT on the Intel or Alpha platforms. Administrator-level privileges to Windows NT are required to install Norton AntiVirus. The Microsoft Exchange service account and password are requested during install.

Platform	Intel or Alpha running Windows NT
Operating systems	Windows NT Server 4.0 with Service Pack 3 or later Windows 2000
Microsoft Exchange	Version 5.0 or 5.5 with latest service packs, Exchange 2000 For VAPI modes, version 5.5 with Service Pack 3 or Exchange 2000 is required (see "Scanning modes" on page 9)
Memory	128 MB RAM
Disk space to install	20 MB
Available disk space for processing	50 MB
Web browser to access Norton AntiVirus	Netscape Navigator (version 4.X or higher) or Internet Explorer (version 4.X or higher), Java, and JavaScript (cookies must be enabled)

Note: It is strongly recommended that servers running Exchange 5.5 Service Pack 3 upgrade to the latest hotfix. Service Pack 3 of Microsoft Exchange has a serious bug when using the Virus API. You should use version 5.5.2651.76 or later. The Exchange information store will not release handles properly and Norton AntiVirus for Microsoft Exchange and the Exchange Information Store will experience problems after several days of operation. See Microsoft Knowledge Base article Q248838 for the latest fixes to Service Pack 3.

Component locations

By default, Norton AntiVirus for Microsoft Exchange components are installed in the following locations:

\Program Files\Navmse	Norton AntiVirus program files
\Program Files\Navmse\Quarantine	Quarantined items in encrypted format
\Program Files\Navmse\Backup	Backed up before repair items in encrypted format
\Program Files\Navmse\Root	User interface files
\Program Files\Navmse\Reports	Reporting data
\Program Files\LiveUpdate	Component to update virus definitions

The following shortcuts are placed in the Norton AntiVirus for Microsoft Exchange group of the Windows Start menu:

- Norton AntiVirus for Microsoft Exchange: Launch the Norton AntiVirus user interface.
- LiveUpdate: Update virus definitions immediately.
- Product Support Online: Access Symantec websites.
- Virus Encyclopedia Online: Review detailed information about known viruses.
- Product Registration: Register Norton AntiVirus for Microsoft Exchange.
- Readme.txt: Review late-breaking news and compatibility information.
- Uninstall: Uninstall Norton AntiVirus for Microsoft Exchange.

In addition, a LiveUpdate properties control panel is placed in the Windows Control Panel group to manually configure the LiveUpdate connection method, if necessary.

Before installing

Before installing, note the following:

- Microsoft Exchange account and password: You will be prompted to enter the account name and password during setup.

  You must have the following User Rights to install:

  - Act as part of the operating system

  - Log on as a service

- Mailbox: During setup, a default mailbox called “NAV for Microsoft Exchange-<server name>” is created. This is the mailbox used by Norton AntiVirus for Microsoft Exchange to send email virus alerts.

  Note: Under Exchange 2000, you must create this mailbox manually before installing.

  You have the option of entering an existing mailbox instead (not necessarily that of an administrator) for an alternate recipient. For example, you may want users to be able to send an email reply to a particular person if they receive a virus alert.

- Microsoft Exchange profile: A profile called “Norton AntiVirus for Microsoft Exchange” is created automatically during setup.

- IP Addresses: During setup, the IP addresses of computers from which Norton AntiVirus for Microsoft Exchange will be accessed are entered. By default, the IP address range for the local network or subnet is used. An access password is also specified during setup.

  For general security, you can use this entire range of IP addresses and rely on the password to restrict access. For maximum security, enter the specific IP addresses of administrators only.

  You can identify the addresses individually and by range. For example,

  ```
  123.12.123.123, 123.12.123.220-123.12.123.255
  ```

  If you are going to administer Norton AntiVirus for Microsoft Exchange from the machine on which it is installed, that machine’s IP address must be included as well.

  Note: To add additional IP addresses after install, you must edit a registry key. See “Granting additional access to Norton AntiVirus for Microsoft Exchange” on page 19 for instructions.

Installing

To install Norton AntiVirus for Microsoft Exchange:

1. Gather the necessary pre-installation information (see the previous section, “Before installing”).
2. Run the Norton AntiVirus for Microsoft Exchange Setup program (SETUP.EXE) and follow the directions in each panel.

On the distribution CD, SETUP.EXE for Norton AntiVirus for Microsoft Exchange is located in the `\Navxchng\Intel` folder for the Intel platform or `\Navxchng\Alpha` folder for the Alpha platform.

3 Note the IP address and port reported for Norton AntiVirus at the end of setup.

After installation, instruct your administrators to point their browsers to this IP address and port to access Norton AntiVirus for Microsoft Exchange.

A shortcut to the user interface is placed in the Start menu of the machine on which you installed Norton AntiVirus.

Installing to Microsoft Exchange cluster servers

Norton AntiVirus for Microsoft Exchange setup is MSCS aware. Setup automatically installs to Microsoft Exchange cluster servers (at the time of this writing only two nodes are supported by MSCS). A few extra steps, however, are required. The next procedures describe how to do the following:

- Install on primary node
- Install on secondary node

To install on the primary node:

1. Run the Norton AntiVirus for Microsoft Exchange Setup program (SETUP.EXE) on the system that is currently hosting Microsoft Exchange in the cluster.
2. In the User Interface Server panel, set the IP address to that of the Cluster IP Address for the Exchange server.
3. In the Remote Access panel, review the settings to ensure the appropriate IP address ranges are allowed access.
4. Complete the setup.

To install on a secondary node:

1. Run the Norton AntiVirus for Microsoft Exchange Setup program (SETUP.EXE) on the system that is acting as the secondary node.
2. Setup should detect that it is being installed on the secondary node, and install the local components of Norton AntiVirus for Microsoft Exchange.
3. Complete the setup.

Scheduling

Norton AntiVirus for Microsoft Exchange uses the NT Schedule service to schedule periodic scans of mailboxes and public folders in MAPI only mode. For all modes, it is used to schedule LiveUpdates of virus definitions. You can configure the Schedule service for Norton AntiVirus use on the cluster server. Note, however, this may affect the operation of other applications and services that use the Schedule service.

To create a Schedule service clustering resource for scheduled scan and scheduled LiveUpdate:

1 Use the Clustering Administrator to create a new clustering resource for the Schedule service in the same group as Microsoft Exchange.

   It should have the following settings:

   - Name: `Schedule`
   - Resource Type: `Generic Service`
   - Dependencies: `Cluster IP Address`
   - Cluster Name
   - Service Name: `Schedule`
   - Use Network Name As Computer Name: Checked

2 Registry Keys: `SYSTEM\CurrentControlSet\Services\Schedule`

3 Complete the New Resource wizard.

In this cluster server configuration, Norton AntiVirus for Microsoft Exchange virus definitions are maintained separately by each node of the cluster. Some effort should be made to keep the virus definitions up-to-date on each node.

One solution is to install NAVNT on each node. Because NAVNT and NAVMSE share virus definitions, NAVNT can be used to schedule LiveUpdates for use by both products. NAVNT does not use the NT schedule service. Additionally, NAVNT provides virus protection for the local files of the node.

Using Norton AntiVirus for Microsoft Exchange

The Norton AntiVirus service, NAV for Microsoft Exchange, is started automatically whenever the server is restarted.

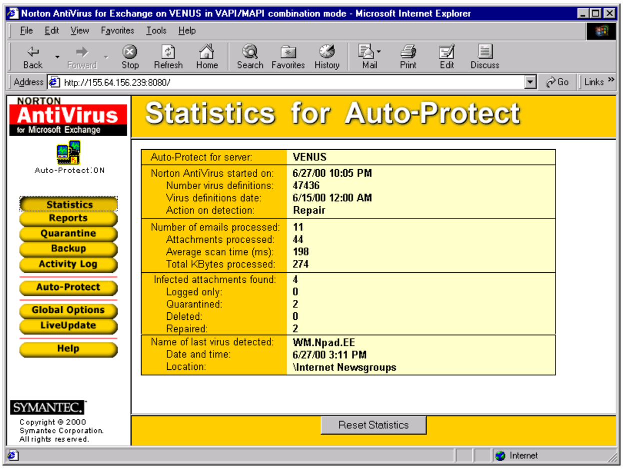
To access the Norton AntiVirus for Microsoft Exchange interface:

1. Do one of the following:
   - Double-click the NAV for Microsoft Exchange shortcut on the Windows desktop.
   - Click the NAV for Microsoft Exchange shortcut in the Windows Start menu.
   - In a browser from any computer on the network, enter the IP address and port where Norton AntiVirus runs (for example, http://127.0.0.1:80). This information was reported during setup.

     The IP address of a remote computer must have been listed during setup. If a machine was not registered during setup, see “Granting additional access to Norton AntiVirus for Microsoft Exchange” on page 19.
2. Enter the password specified during setup.

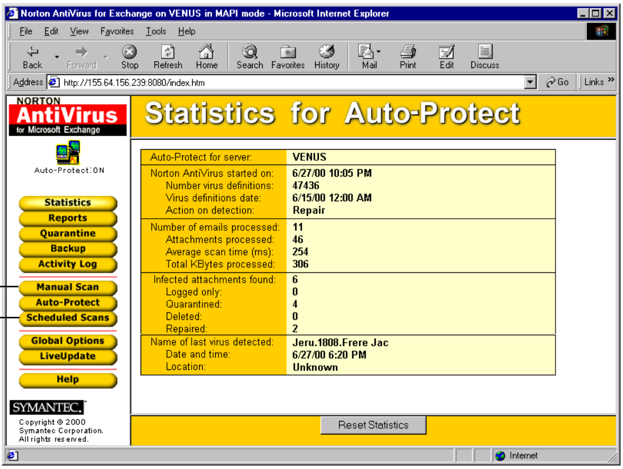
   Although the browser asks for a user name, only the password is required. The user name is ignored.

MAPI/VAPI combination mode


Norton AntiVirus for Exchange on VENUS in VAPI/MAPI combination mode - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Discuss
Address
http://155.64.156.239:8080/
Go
Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Statistics for Auto-Protect
Reset Statistics
Internet

Auto-Protect for server:	VENUS
Norton AntiVirus started on:	6/27/00 10:05 PM
Number virus definitions:	47436
Virus definitions date:	6/15/00 12:00 AM
Action on detection:	Repair
Number of emails processed:	11
Attachments processed:	44
Average scan time (ms):	198
Total KBytes processed:	274
Infected attachments found:	4
Logged only:	0
Quarantined:	2
Deleted:	0
Repaired:	2
Name of last virus detected:	WM.Npad.EE
Date and time:	6/27/00 3:11 PM
Location:	\Internet Newsgroups

MAPI only mode


Norton AntiVirus for Exchange on VENUS in MAPI mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Discuss
Address http://155.64.156.239:8080/index.htm
Go
Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Manual Scan
Auto-Protect
Scheduled Scans
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Reset Statistics
Internet

Statistics for Auto-Protect

Auto-Protect for server:	VENUS
Norton AntiVirus started on:	6/27/00 10:05 PM
Number virus definitions:	47436
Virus definitions date:	6/15/00 12:00 AM
Action on detection:	Repair
Number of emails processed:	11
Attachments processed:	46
Average scan time (ms):	254
Total KBytes processed:	306
Infected attachments found:	6
Logged only:	0
Quarantined:	4
Deleted:	0
Repaired:	2
Name of last virus detected:	Jeru.1808.Frere Jac
Date and time:	6/27/00 6:20 PM
Location:	Unknown

Manual and Scheduled Scans available in MAPI only mode

There are three primary Norton AntiVirus operations: reporting, scanning, and configuration.

Reporting

- Statistics: Summaries of Auto-Protect processing, virus detections, and Norton AntiVirus status.
- Reports: Detections ordered by author, scan type, or virus, can be sorted by month or year. Raw data can also be downloaded in comma-delimited format (.CSV).
- Quarantine: Infected attachments that have been stripped from emails and messages.
- Backup: Copies of attachments backed up before a repair is attempted.
- Activity Log: Server events including Auto-Protect, virus detections, LiveUpdate, and services. In MAPI mode, Manual and Scheduled Scans information is included.

Scanning

- Auto-Protect: Detects viruses in realtime, before they have a chance to spread through the site. Auto-Protect is the best defense against virus attack.

  In VAPI or MAPI/VAPI mode, Auto-Protect includes background scans of the Exchange information store that replace manual and scheduled scans.

- Manual Scan (MAPI mode only): Scans of mailboxes and public folders on demand.
- Scheduled Scans (MAPI mode only): Scans that run unattended, usually at off-peak periods, to ensure that your Microsoft Exchange servers remain virus-free. The Windows NT Scheduler service must be running.

Configuration

- Global Options: Optimize Auto-Protect, Manual Scan (MAPI mode), and future Scheduled Scans (MAPI mode). Set notifications, logging, reporting, and Quarantine server options. The default settings are appropriate for most sites.
- LiveUpdate: Set the frequency at which updated virus definitions files are automatically downloaded and installed to ensure protection against newly discovered viruses.

Changing scanning modes

Norton AntiVirus for Microsoft Exchange operates in three different modes:

- MAPI/VAPI combination mode: Uses the latest antivirus technology (VAPI), including full-featured logging and reporting capability. Recommended for most installations.
- VAPI mode: Uses the latest antivirus technology (VAPI), but logging and reporting capabilities are reduced. Recommended when server performance is critical.
- MAPI mode: Provides virus protection using existing antivirus technology, but includes full-featured logging and reporting capability.

See “Scanning modes” on page 9 for more information.

To change modes after installation:

1. In the left panel, click Auto-Protect.
2. On the mode tab, select the preferred operating mode and click Switch Mode.

Granting additional access to Norton AntiVirus for Microsoft Exchange

As a security precaution, Norton AntiVirus can only be accessed from machines whose IP addresses were entered during setup. To add additional machines after setup, you must modify a registry key on the machine on which Norton AntiVirus is installed:

```
HKEY_LOCAL_MACHINE\Software\Symantec\
NAVMSE\2.1\ModifyIPaddrs
```

You can identify the addresses individually and by range. For example,

```
123.12.123.123, 123.12.123.220-123.12.123.255
```

After making changes, stop and restart the NAV for Microsoft Exchange service.

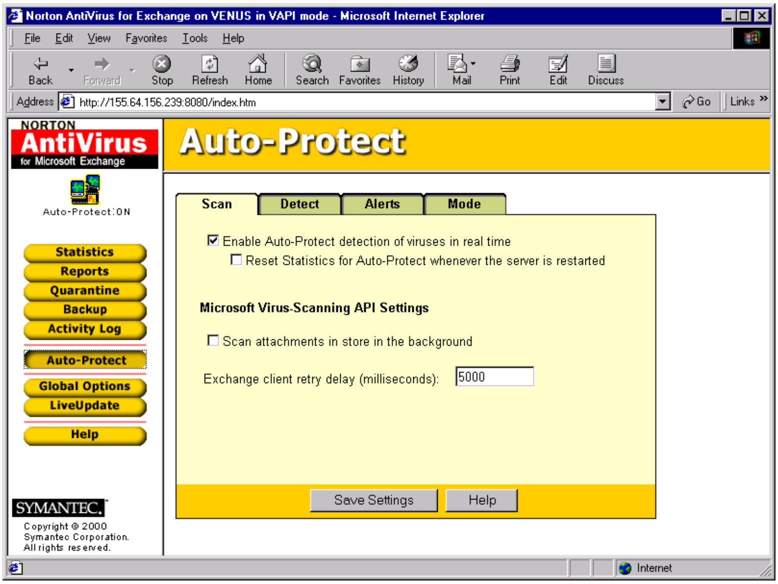
Scanning for viruses: VAPI and MAPI/VAPI combination modes

This section describes scanning in VAPI and MAPI/VAPI combination modes. See "Scanning for viruses: MAPI only mode" on page 23 for information about MAPI only mode.

All scanning in the VAPI and MAPI/VAPI combination modes is performed by Auto-Protect. Three aspects are configured: Scan, Detect, and Alerts.

To configure Auto-Protect:

1 In the Norton AntiVirus window, click Auto-Protect.


Norton AntiVirus for Exchange on VENUS in VAPI mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://155.64.156.239:8080/index.htm
Go Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Auto-Protect
Scan
Detect
Alerts
Mode
Save Settings
Help
Internet

☑ Enable Auto-Protect detection of viruses in real time

☐ Reset Statistics for Auto-Protect whenever the server is restarted

Microsoft Virus-Scanning API Settings

☐ Scan attachments in store in the background

Exchange client retry delay (milliseconds): 5000

2 Specify settings on the Scan, Detect, and Alerts tabs. Click the Save Settings button on each tab after making changes.

Scan settings

Scan: Enable Auto-Protect

- Check to enable Auto-Protect operation. With VAPI, every attachment is scanned before it can be accessed by a user.
- To supplement Auto-Protect, check Scan All Attachments In Store In The Background. Because all items in the Exchange information store are scanned, manual and scheduled scans are not required for complete protection.

Detect: What to do if a virus is detected

- Log Only: The detection is entered in the log and the email or message is delivered with the infected attachment.
- Quarantine: The infected attachment is stripped and the email or message is delivered. The attachment is replaced with a text notification. Click Quarantine to view or delete quarantined items. See "Managing reports" on page 35 for information on using the Quarantine. The attachment is replaced with a text notification.
- Delete: Infected attachments are simply stripped and deleted. The attachment is replaced with a text notification. The remainder of the email or message is delivered.
- Repair: The virus is eliminated from the attachment and delivery is continued. Norton AntiVirus for Microsoft Exchange detects and eliminates viruses within compressed files, such as ZIP and encoded MIME formats.

  If for any reason the attachment cannot be repaired, you can specify an alternative option: Log Only, Delete, or Quarantine.

Alerts: Whom to notify if a virus is detected

- Emails: Specify who is notified of the virus detection. If your options are set to Delete or Quarantine, this may be the only time users are apprised that something is missing from the email or message.
- Alerts: Specify users and machines to receive Windows NT alerts on virus detections. If Norton AntiVirus for Windows NT Servers is running on the network, alerts can be sent to its alert service as well.

Mode: Switch scan modes

- Select the Norton AntiVirus scanning mode: MAPI/VAPI, VAPI, or MAPI. See “Scanning modes” on page 9 for more information.

Scanning for viruses: MAPI only mode

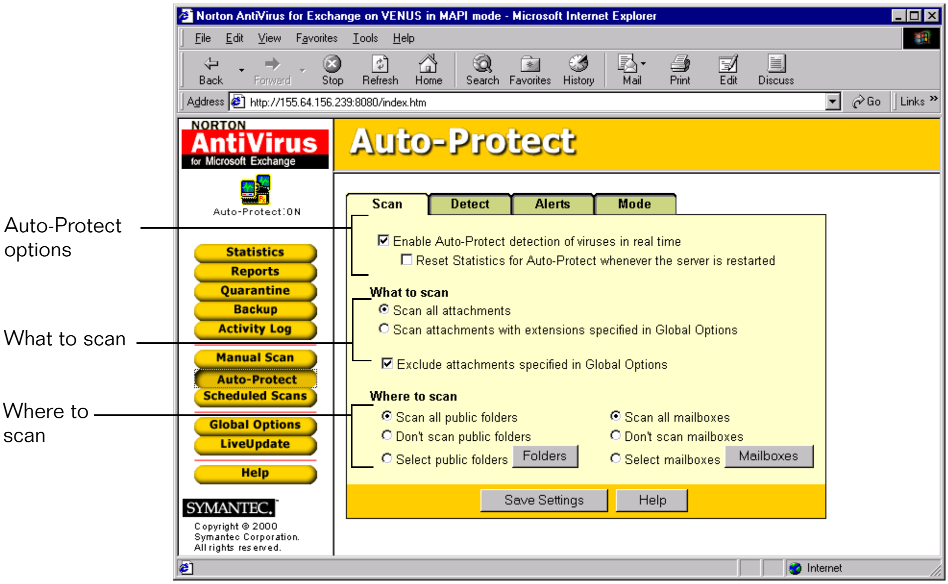
This section describes scanning in MAPI only mode. See "Scanning for viruses: VAPI and MAPI/VAPI combination modes" on page 20 for information about VAPI and MAPI/VAPI combination modes.

The procedure to implement each Norton AntiVirus scan type in MAPI mode is essentially the same, with three tabs for each scan type: Scan, Detect, and Alerts. Auto-Protect has additional check boxes to enable or disable protection and reset processing statistics. Scheduled Scans has an additional tab to set the scan frequency.

Note: To be scanned, public folders and mailboxes must reside on the Microsoft Exchange server.

To configure scans:

1 In the Norton AntiVirus window, click a scan type in the left panel: Manual Scan, Auto-Protect, or Scheduled Scans.


Norton AntiVirus for Exchange on VENUS in MAPI mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://155.64.156.239:8080/index.htm
Go Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Manual Scan
Auto-Protect
Scheduled Scans
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Auto-Protect
Scan
Detect
Alerts
Mode
Folders
Mailboxes
Save Settings
Help
Internet

☑ Enable Auto-Protect detection of viruses in real time

□ Reset Statistics for Auto-Protect whenever the server is restarted

What to scan

● Scan all attachments

○ Scan attachments with extensions specified in Global Options

☑ Exclude attachments specified in Global Options

Where to scan

● Scan all public folders
○ Don't scan public folders
○ Select public folders

● Scan all mailboxes
○ Don't scan mailboxes
○ Select mailboxes

Auto-Protect options

What to scan

Where to scan

Note: For Scheduled Scans, click Add Scan in the list of scheduled scans to schedule a new scan. Select an existing scan and click Edit to modify it. The Windows NT Schedule service must be running for scheduled scans to occur. If the Schedule service is not running, the list of scheduled scans is not displayed. You can still click Add Scan to schedule scans.

2. Specify settings on the Scan, Detect, and Alerts tabs. Click the Save Settings button on each tab after making changes.

   See “Scan settings” on page 21 for information about the settings.

3. Enable the scan. Do one of the following:

   - Manual Scan

     After the scan is configured, click the Scan Now button at the bottom of the Scan tab to begin the scan.

   - Auto-Protect

     Use the Enable Auto-Protect check box on the Scan tab to turn real-time protection on or off.

   - Scheduled Scans

     Click the Add To Schedule button on the Schedule tab to return to the display of scheduled scans.

Scan settings

Scan: What and where to scan

- Scan all attachments or specified attachments: To reduce resource demand, you can instruct Norton AntiVirus for Microsoft Exchange to scan only attachments likely to become infected. The default list of file extensions, set in Global Options, contains most file types at risk. If you encounter executable files with unusual extensions, you can add them to the list.
- Exclude specified extensions: Also identified in Global Options, attachments with these extensions are not scanned. Exclusions take precedence over Scan All or Scan Specified Attachments settings. An excluded item is never scanned.
- Specify which specific public folders and mailboxes to scan.

Detect: What to do if a virus is detected

- Log Only: The detection is entered in the log and the email or message is delivered with the infected attachment.
- Quarantine: The infected attachment is stripped and the email or message is delivered. The attachment is replaced with a text notification. Click Quarantine to view or delete quarantined items. See "Managing reports" on page 35 for information on using the Quarantine.
- Delete: Infected attachments are simply stripped and deleted. The attachment is replaced with a text notification. The remainder of the email or message is delivered.
- Repair: The virus is eliminated from the attachment and delivery is continued. Norton AntiVirus for Microsoft Exchange detects and eliminates viruses within compressed files, such as ZIP and encoded MIME formats.

  If for any reason the attachment cannot be repaired, you can specify an alternative option: Log Only, Delete, or Quarantine.

Alerts: Whom to notify if a virus is detected

- Emails: Specify whether administrators, intended recipients, or senders of the email or message are notified of the virus detection. If your options are set to Delete or Quarantine, this may be the only time users are apprised that something is missing from the email or message.
- Alerts: Specify users and machines to receive Windows NT alerts on virus detections. If Norton AntiVirus for Windows NT Servers is running on the network, alerts can be sent to its alert service as well.

Mode: Switch scan modes

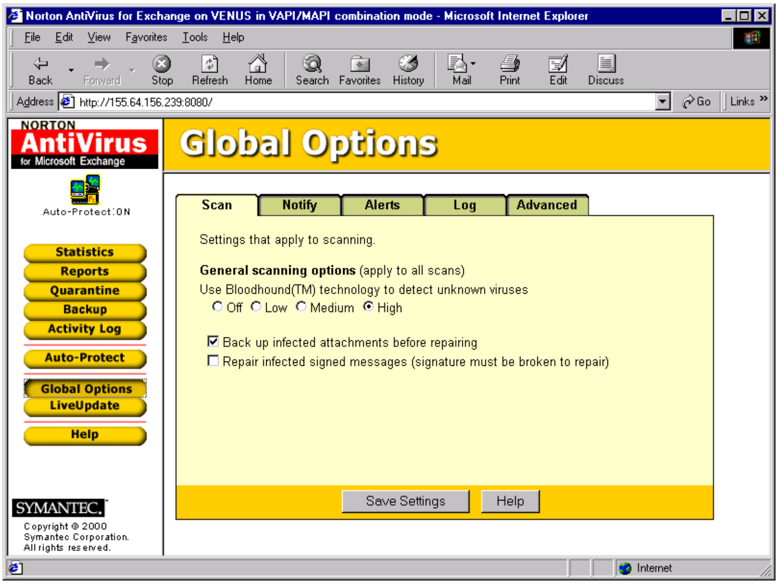
- Select the Norton AntiVirus scanning mode: MAPI/VAPI, VAPI, or MAPI. See "Scanning modes" on page 9 for more information.

Setting Global Options

Global Options apply to all scan types. If a setting is changed, it affects whatever is selected in Auto-Protect, and Manual and future Scheduled Scans in MAPI only mode. See "Scanning modes" on page 9 for a summary of the differences among the modes.

Note: All screens display the default global options.

Global Options: Scan (VAPI and MAPI/VAPI combination modes)


Norton AntiVirus for Exchange on VENUS in VAPI/MAPI combination mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://155.64.156.239:8080/
Go Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Global Options
Scan
Notify
Alerts
Log
Advanced
Save Settings
Help
Internet

Settings that apply to scanning.

General scanning options (apply to all scans)

Use Bloodhound(TM) technology to detect unknown viruses

○ Off ○ Low ○ Medium ● High

☑ Back up infected attachments before repairing

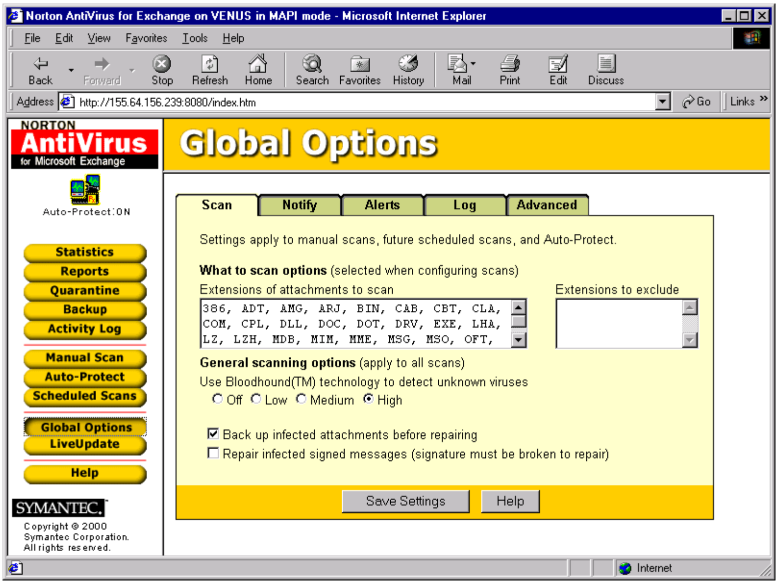
□ Repair infected signed messages (signature must be broken to repair)

- Use Bloodhound virus detection technology: To supplement detection of known viruses, Norton AntiVirus can detect a high percentage of new or unknown viruses not yet analyzed by antivirus researchers. The Medium setting optimizes processing. In a high-risk environment, increase to High.
- Back up attachments before repairing: For additional security, Norton AntiVirus can make a backup copy of an infected attachment before attempting to eliminate a virus. There is a slight increase in processing time with this option.

Backed up files are stored in a Backup directory that is created in the NAVMSE directory during setup. To release files, click Backup in the left panel, then click Release To File System. They are released to the Backup\Release directory.

- Repair signed messages: Norton AntiVirus can scan signed messages for viruses. However, if you specify the Repair option when configuring the various scan types, the signature must be violated to make the repair.

Global Options: Scan (MAPI only mode)



Settings apply to manual scans, future scheduled scans, and Auto-Protect.

What to scan options (selected when configuring scans)

Extensions of attachments to scan

```
386, ADT, AMG, ARJ, BIN, CAB, CBT, CLA,
COM, CPL, DLL, DOC, DOT, DRV, EXE, LHA,
LZ, LZH, MDB, MIM, MME, MSG, MSO, OFT,
```

Extensions to exclude

General scanning options (apply to all scans)

Use Bloodhound(TM) technology to detect unknown viruses

○ Off ○ Low ○ Medium ● High

☑ Back up infected attachments before repairing

☐ Repair infected signed messages (signature must be broken to repair)

- Attachments to scan: To reduce resource demand when setting the various scan options, you can instruct Norton AntiVirus to scan only attachments likely to become infected. The default list of file extensions contains most file types at risk. If you encounter executable files with unusual extensions, you can add them to the list.
- Files and extensions to exclude from scans: If selected when setting the various scan options, attachments with these extensions are not scanned. Exclusions take precedence over other scan settings. An excluded item is never scanned.
- Use Bloodhound virus detection technology: To supplement detection of known viruses, Norton AntiVirus can detect a high percentage of new or unknown viruses not yet analyzed by antivirus researchers. The

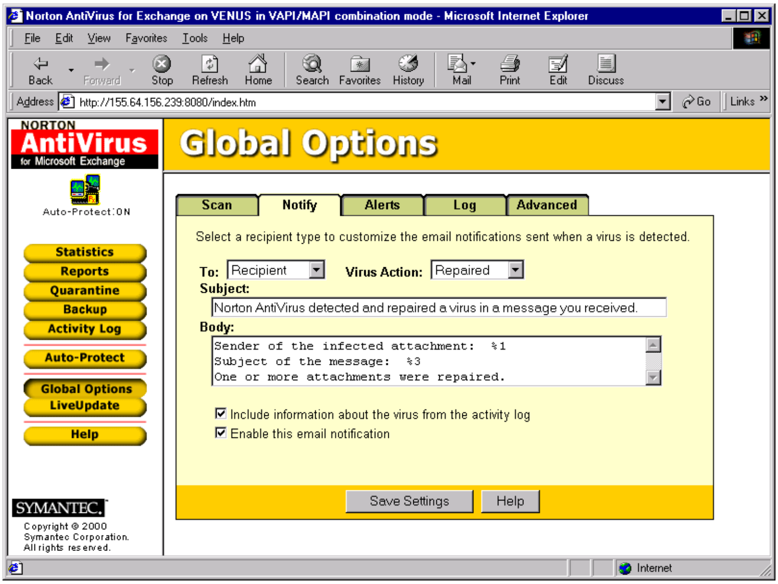
Medium setting optimizes processing. In a high-risk environment, increase to High.

- Back up attachments before repairing: For additional security, Norton AntiVirus can make a backup copy of an infected attachment before attempting to eliminate a virus. There is a slight increase in processing time with this option.

  Backed up files are stored in a Backup directory that is created in the NAVMSE directory during setup. To release files, click Backup in the left panel, then click Release To File System. They are released to the Backup\Release directory.

- Repair signed messages: Norton AntiVirus can scan signed messages for viruses. However, if you specify the Repair option when configuring the various scan types, the signature must be violated to make the repair.

Notify options


Norton AntiVirus for Exchange on VENUS in VAPI/MAPI combination mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Go Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Global Options
Scan
Notify
Alerts
Log
Advanced
Save Settings
Help
Internet

Address http://155.64.156.239:8080/index.htm

Select a recipient type to customize the email notifications sent when a virus is detected.

To: Recipient   Virus Action: Repaired

Subject: Norton AntiVirus detected and repaired a virus in a message you received.

Body:

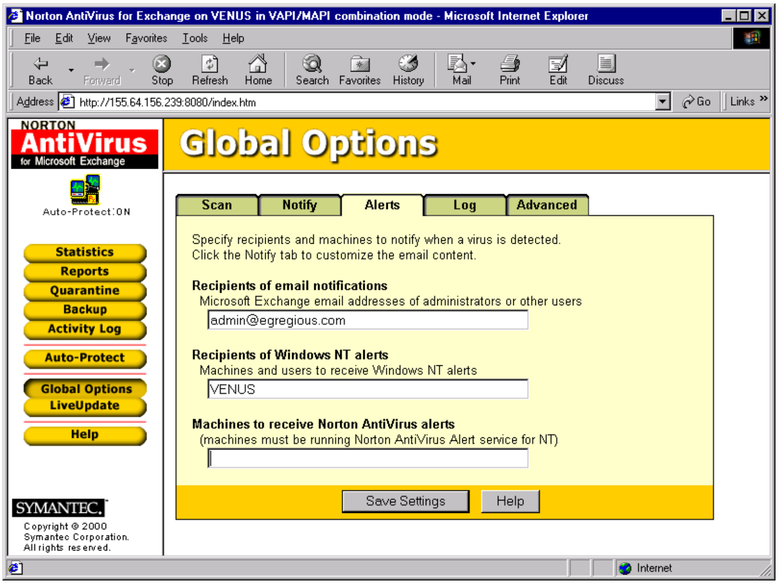
```
Sender of the infected attachment:  %1
Subject of the message:  %3
One or more attachments were repaired.
```

☑ Include information about the virus from the activity log

☑ Enable this email notification

Customize the content of email alerts sent to administrators, intended recipients, and message authors when a virus is detected. You can have different subjects and content for each group. For example, for message authors you may want to identify an MIS technician users can contact for more information or describe a procedure to run a workstation scan with a local version of Norton AntiVirus.

Alerts options


Norton AntiVirus for Exchange on VENUS in VAPI/MAPI combination mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://155.64.156.239:8080/index.htm
Go Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Global Options
Scan
Notify
Alerts
Log
Advanced
Save Settings
Help
Internet

Specify recipients and machines to notify when a virus is detected.
Click the Notify tab to customize the email content.

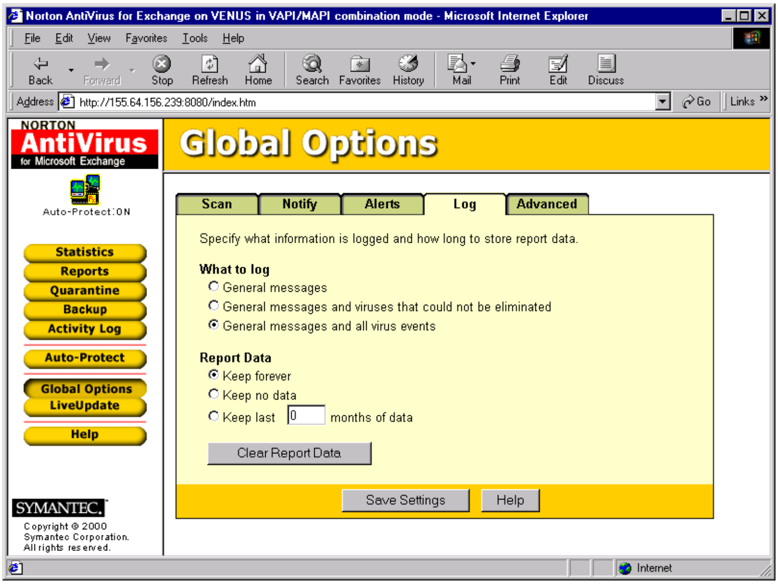
Recipients of email notifications
Microsoft Exchange email addresses of administrators or other users
admin@egregious.com

Recipients of Windows NT alerts
Machines and users to receive Windows NT alerts
VENUS

Machines to receive Norton AntiVirus alerts
(machines must be running Norton AntiVirus Alert service for NT)

List the email addresses of administrators, machines, and users to receive Windows NT alerts, and machines running Norton AntiVirus for Windows NT Servers. In each case, separate entries with semicolons. Do not include spaces after the semicolon.

Log options


Norton AntiVirus for Exchange on VENUS in VAPI/MAPI combination mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://155.64.156.239:8080/index.htm
Go Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Global Options
Scan
Notify
Alerts
Log
Advanced
Clear Report Data
Save Settings
Help
Internet

Specify what information is logged and how long to store report data.

What to log

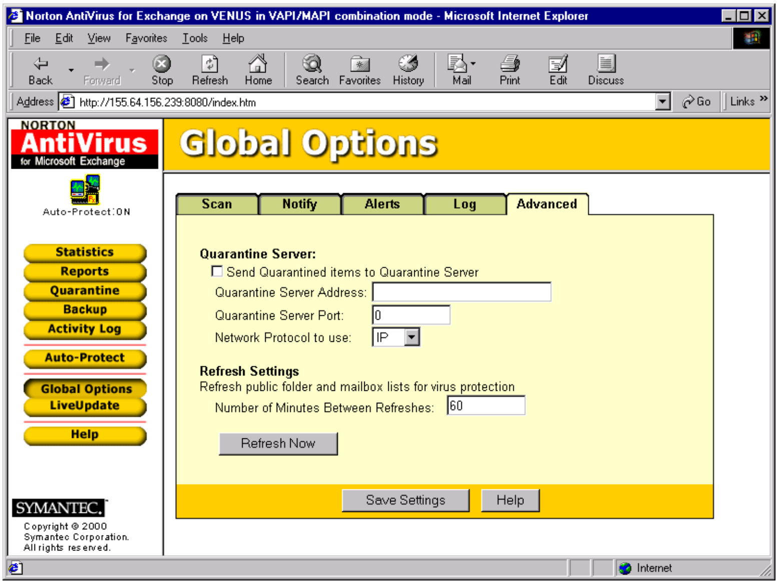
○ General messages
○ General messages and viruses that could not be eliminated
● General messages and all virus events

Report Data

● Keep forever
○ Keep no data
○ Keep last 0 months of data

Specify what to log. The Norton AntiVirus activity log is viewed through the HTML interface. You can set how long Norton AntiVirus keeps data for the activity log. In addition, all events are stored in the Windows NT application log, viewed with the Windows NT event viewer.

Advanced options


Norton AntiVirus for Exchange on VENUS in VAPI/MAPI combination mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://155.64.156.239:8080/index.htm
Go Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Global Options
Scan
Notify
Alerts
Log
Advanced
Refresh Now
Save Settings
Help
Internet

Quarantine Server:

□ Send Quarantined items to Quarantine Server

Quarantine Server Address:

Quarantine Server Port: 0

Network Protocol to use: IP

Refresh Settings

Refresh public folder and mailbox lists for virus protection

Number of Minutes Between Refreshes: 60

If a Norton AntiVirus Central Quarantine server is created as part of enterprise-wide antivirus protection managed by the Symantec System Center, items can be forwarded automatically from the Norton AntiVirus for Microsoft Exchange Quarantine to the Central Quarantine. Specify the IP address and listening port set when configuring the centralized Quarantine and the appropriate network protocol. See your Symantec System Center documentation for more information.

Refresh Settings determine how frequently Norton AntiVirus checks for newly created folders and mailboxes.

Maintaining current protection

Norton AntiVirus relies on up-to-date information to detect and eliminate viruses. One of the most common reasons virus problems occur is that virus definitions files are not updated after installation. Symantec regularly supplies updated virus definitions files that contain the necessary information about all newly discovered viruses.

About LiveUpdate

With LiveUpdate, Norton AntiVirus connects automatically to special Symantec sites and determines if virus definitions need updating. If so, it downloads the proper files and installs them in the proper location.

LiveUpdate also checks for and downloads program patches to Norton AntiVirus for Microsoft Exchange, if available. An email is sent to administrators specified in Global Options with the location of the patch. Program modifications are never made outside of administrator control.

Generally, you do not have to do anything to configure LiveUpdate. The only requirement is an Internet connection. If necessary, you can configure LiveUpdate operation.

To configure LiveUpdate operation:

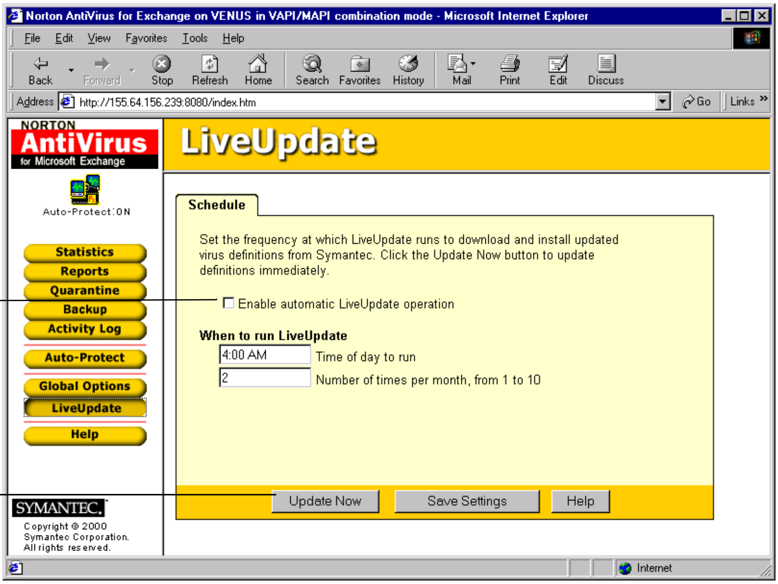
1. Open the Windows NT Control Panel.
2. Double-click LiveUpdate.
3. Modify your settings in LiveUpdate Properties.

   The LiveUpdate online help explains all options.

How to update virus protection

To schedule automatic LiveUpdates:

1 In the Norton AntiVirus for Microsoft Exchange main window, click LiveUpdate.


Norton AntiVirus for Exchange on VENUS in VAPI/MAPI combination mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://155.64.156.239:8080/index.htm
Go Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
LiveUpdate
Schedule
Update Now
Save Settings
Help
Internet

Set the frequency at which LiveUpdate runs to download and install updated virus definitions from Symantec. Click the Update Now button to update definitions immediately.

☐ Enable automatic LiveUpdate operation

When to run LiveUpdate

4:00 AM Time of day to run

2 Number of times per month, from 1 to 10

Check to enable the scheduled LiveUpdate

Click to run LiveUpdate immediately

2 In the Schedule section of the form, check Enable LiveUpdate.

If you choose to disable automatic operation, make it a practice to click the Update Now button regularly.

3 Enter the number of times per month for LiveUpdate to run.

A month is considered to be 28 days. The initial LiveUpdate runs on a random day during the month. The next runs 28/n days later.

4 Enter the time of day that LiveUpdate runs.

Specify an off-peak time in a high-traffic network.

Updating virus protection without LiveUpdate

Symantec provides the latest virus definitions files with a program called Intelligent Updater, available for download from the Symantec website (http://www.symantec.com) and other sources listed in the Service and Support Solutions in this guide.

To update virus definitions files:

1 Download (or copy) Intelligent Updater to any directory on the server.

2 Run Intelligent Updater.

Intelligent Updater reads the Windows NT registry and installs the necessary files in the proper locations.

3 Delete the downloaded Intelligent Updater program.

Managing reports

Once configured, Norton AntiVirus runs quietly and vigilantly in the background. Although you access the program to view Statistics, examine the Activity Log, and manage the Quarantine of infected items, the only real requirement is to update virus definitions regularly.

Statistics

Provides a live report of Norton AntiVirus Auto-Protect operation. General metrics show how efficiently the scanning runs on your server.

Reports

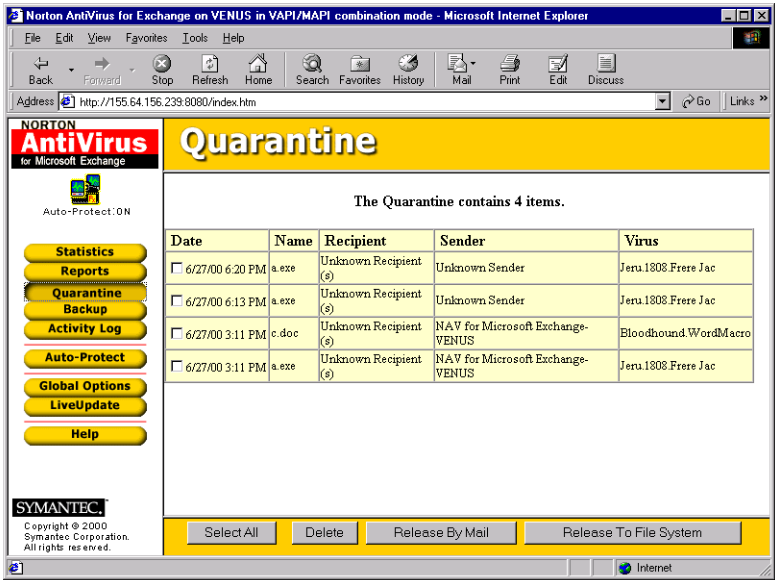
Provides summaries of virus detections. The detections can be ordered by author, scan type, or virus, and restricted to month or year. For display by other applications, the raw data can also be downloaded in comma-delimited format (.CSV).

Quarantine

Stores virus-infected attachments detected during scans. Attachments are placed in the Quarantine under three circumstances:

- A virus is detected in an attachment and your scan is configured to withhold delivery rather than let Norton AntiVirus repair or delete the infected attachment.
- Your scan is configured to let Norton AntiVirus repair infected attachments, and Quarantine is selected for the attachments that can’t be repaired. Sometimes attachments can’t be properly restored because they are corrupted or damaged by a virus that causes irreversible damage.

- If an item can’t be scanned, it is quarantined by default. For example, an item my be compressed and password-protected.


Norton AntiVirus for Exchange on VENUS in VAPI/MAPI combination mode - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Discuss
Address http://155.64.156.239:8080/index.htm
Go
Links
NORTON AntiVirus for Microsoft Exchange
Auto-Protect:ON
Statistics
Reports
Quarantine
Backup
Activity Log
Auto-Protect
Global Options
LiveUpdate
Help
SYMANTEC.
Copyright © 2000 Symantec Corporation. All rights reserved.
Quarantine
Select All
Delete
Release By Mail
Release To File System
Internet

The Quarantine contains 4 items.

Date	Name	Recipient	Sender	Virus
□ 6/27/00 6:20 PM	a.exe	Unknown Recipient (s)	Unknown Sender	Jeru.1808.Frere Jac
□ 6/27/00 6:13 PM	a.exe	Unknown Recipient (s)	Unknown Sender	Jeru.1808.Frere Jac
□ 6/27/00 3:11 PM	c.doc	Unknown Recipient (s)	NAV for Microsoft Exchange-VENUS	Bloodhound.WordMacro
□ 6/27/00 3:11 PM	a.exe	Unknown Recipient (s)	NAV for Microsoft Exchange-VENUS	Jeru.1808.Frere Jac

Infected items are held in the Quarantine for administrator review. You can delete or release the quarantined items from within Norton AntiVirus for Microsoft Exchange.

Quarantined files are encrypted and stored in a Quarantine directory that is created in the NAVMSE directory during setup. To release files, click Quarantine in the left panel, then click Release To File System. They are released to the Quarantine\Release directory.

Click Release By Mail to release the item to the intended recipient. If the recipient is not known, it is sent to administrators identified on the Alerts tab of Global Options. Note that if an item is released by mail, the the scan policy in force will apply to the item. If infected, it will be detected again.

Backup

For data security, Norton AntiVirus can make an encrypted backup copy of a file before attempting a repair. The files are stored in a Backup directory that is created in the NAVMSE directory during setup.

After verifying that the virus-infected files were successfully repaired, delete them. If necessary, you can release the backed up files. Click Release To File System. They are released to the Backup\Release directory.

Activity Log

By default, records all virus, configuration, and server events. The log lists entries in chronological order beginning with the most current event at the top. You can specify dates of interest as well as filter the log to display specific events.

In the Log tab of Global Options, you can specify which events to record to the Windows NT event log.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers several technical support options:

- StandardCare support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, then select your product and version. This gives you access to product knowledge bases, interactive troubleshooter, Frequently Asked Questions (FAQs), and more.

- PriorityCare, GoldCare, and PlatinumCare support

  Fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

  For telephone support information, connect to http://service.symantec.com, select your product and version, and click Contact Customer Support.

- Automated fax retrieval

  Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 984-2490.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for six months after the release of the new version. Technical information may still be available through the Service & Support Web site (http://service.symantec.com).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Visit Symantec Customer Service online at http://www.symantec.com/techsupp/news/custserv.html for assistance with non-technical questions and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at: http://www.symantec.com/upgrades/ or call the Customer Service Order Desk at (800) 568-9501.

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://www.symantec.com, select the country you want information about, and click Go!

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401

http://www.symantec.com/
(Fax: (541) 984-8020

Automated Fax Retrieval
(800) 554-4403
(541) 984-2490

Argentina, Chile, and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.symantec.com/region/mx
+54 (11) 4315-0889
Fax: +54 (11) 4314-3434

Asia/Pacific Rim

Symantec Australia Pty. Ltd.
408 Victoria Road
Gladesville, NSW 2111
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 9850 1000
Fax: +61 (2) 9817 4550

Brazil

Symantec Brazil
Av. Juruce, 302 - cj 11
São Paulo - SP
04080 011
Brazil

http://www.symantec.com/region/br/
+55 (11) 531-7577
Fax: +55 (11) 5530 8869

Columbia, Venezuela, the Caribbean, and Latin America

Symantec América Latina
2501 Colorado, Suite 300
Santa Monica, CA 90404

http://www.symantec.com/region/mx/
+1 (541) 334-6050 (U.S.A.)
Fax: (541) 984-8020 (U.S.A.)

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032
Fax: +353 (1) 811 8033

Automated Fax Retrieval
+31 (71) 408-3782

Mexico

Symantec Mexico
Periferico Sur No. 3642, Piso 14
Col. Jardines del Pedregal
09100 Mexico, D.F.

http://www.symantec.com/region/mx
+52 (5) 661-6120; +1 (800) 711-8443
Fax: +52 (5) 661-8819

Virus protection subscription policy

If your Symantec product includes virus protection, you might be entitled to receive free virus protection updates via LiveUpdate. The length of the free subscription could vary by Symantec product.

When you near the end of your virus protection subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your free subscription ends, you must renew your subscription before you can update your virus protection. Renewal subscriptions are available for a nominal charge.

To order a subscription, do one of the following:

- Visit our Web site at: http://www.shop.symantec.com.
- Outside the United States, contact your local Symantec office or representative.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

May 2000

Norton AntiVirus™ for Microsoft Exchange
CD Replacement Form

DISK REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form and 2) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement disks. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive disk replacements.

FOR CD REPLACEMENT

Please send me: ___ CD (replacement)

Name ____

Company Name ______________________________________

Street Address (No P.O. Boxes, Please)______________________

City ______________________________ State _______ Zip/Postal Code ______________

Country* ____________________________Daytime Phone ____________________

Software Purchase Date ______________________________

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem:______________________________

____

Disk Replacement Price	$ 10.00
Sales Tax (See Table)	______
Shipping & Handling	$ 9.95
TOTAL DUE	______

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _________ __ Visa __ Mastercard __ American Express

Credit Card Number ______________________________Expires _________

Name on Card (please print) ____________________ Signature ____________________

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003
Please allow 2-3 weeks for delivery within the U.S.

INDEX